DEPARTMENT OF THE AIR FORCE
HQ AIR INTELLIGENCE AGENCY

AIA RECURRING PERIODICAL 31-1

3rd Quarter 2000

Security

THE SHIELD

OPR: HQ AIA/SOCD (MSgt Guy Woodbury) Certified by: HQ AIA/SOC (Mr. Robert Eddy)
Pages: 7
Distribution: F

FOREWORD This recurring publication is published quarterly to assist security managers administer unit security training and education programs. It supports the Air Intelligence Agency (AIA) Security Training, Education, and Motivation (STEM) Program governed by AIA Supplement 1 to AFI 31-401, *Managing The Information Security Program*. The contents are for information and training purposes only. Articles presented herein do not represent a change of policy or requirements unless officially incorporated into Air Force or Agency instructions.

We solicit your suggestions for articles or other ideas for publication. We are very interested in "cross-feeding" improved methods, effective procedures, quality enhancements, or other publications and training aids in this publication. Please forward any articles or suggested topics to the Security Information Division, Disclosure Branch, HQ AIA/SOCD, 102 Hall Blvd, Suite 257, San Antonio TX 78243-7026 or e-mail: guy.woodbury@kelly.af.mil.

1. INFORMATION SECURITY.

1.1. FOREIGN TRAVEL AND SECURITY BRIEFINGS by MSgt Steve Kramer, HQ AIA/SOCD.

Did you know personnel with access to Sensitive Compartmented Information (SCI) are required to notify their SCI security officials (normally their security manager) of official and unofficial travel to all foreign countries? Yes, there is such a policy, and it includes travel to Mexico and Canada. However, reporting the travel is only the first step.

The second step is to receive a foreign travel briefing. This briefing is usually given by security managers and is intended to alert the traveler of the potential threats from harassment, exploitation, capture, entrapment, or criminal activity. These briefings will also include courses of action to mitigate these situations.

Because you have access to classified information, you are a potential target for foreign intelligence agents. As a traveler, you are more vulnerable because you may be unfamiliar with the customs, people, language, and laws of that country. You become more dependent upon strangers. This is an

attractive situation for the foreign agent. The same opportunities exist in both "friendly" and "unfriendly" countries. Be alert to overly friendly or helpful strangers. Do not fall into a compromising situation where outside help may be needed or threats of blackmail could surface.

If you suspect someone may be attempting to gather classified or other sensitive information from you, report it to your local SCI security officials and supporting counterintelligence agency.

Be a smart traveler. Carry personal identification and any special medical information with you at all times. Store essential medication in original containers. Do not leave your wallet or purse unattended. Leave your itinerary with your SCI security officials and advise them of any changes to your itinerary during your trip.

If you should find yourself needing assistance while traveling, contact the Department of State's Citizens Emergency Center at (202 647-5225). Current country and threat information, to include threat advisories, can be found on the worldwide web at http://travel.state.gov.

If you follow a few basic precautions, you will reduce your risk of encountering problems while in a foreign country.

1.2. MESSAGES TO THE FIELD by MSgt Steve Kramer, HQ AIA/SOCD.

The following messages are from the past quarter and contain policy or guidance from HQ AIA/SO and others. They are intended for use throughout the Agency and supported element security offices; however, some apply only to the Wings, Groups, and Centers. If your organizations is not in receipt of, or on distribution for a below message, forward your inquiry to Mrs. Darleen Benware at DSN: 969-2888 or darleen.benware@kelly.af.mil.

JGUBY MESSAGES: Used to disseminate security information to AIA units.

JGUBY 00-10, 211632Z Jun 00, Classified in Open Source.

NOSIZ MESSAGES: Used to disseminate security training information.

NOSIZ 00-06, 221502Z May 00, SCIF Accreditation and DIA Compartmented Address Book HCS Updates.

NOSIZ 00-07, 191754Z Jun 00, USAF SCI Security Management Course Info.

NOSIZ 00-08, 141403Z Jul 00, USAF SCI Management Course Info.

ODANS MESSAGES: Used to disseminate SCI Policy to USAF SSOs.

ODANS 00-02, 110236Z May 00, HCS Security Manual Clarification.

ROXAD MESSAGES: Used to disseminate updates and clarification of policy to the field.

ROXAD 00-02 (SSO AIA), 221919Z May 00, SCIF Accreditation and Compartmented Address Book HCS Updates.

ROXAD 00-03 (SSO USAF/XOIIS), 171355Z Jul 00, DIA SCI Security Officials Course.

AIG 8551: Used to disseminate information to AIA Security Forces.

AIG 8551 00-04, 081555Z Jun 00, 3P051 CDC Volume 2 Replacement.

AIG 8551 00-05, 061922Z Jul 00, Information Security Management Information Systems (MIS) Data Report.

AIG 8551 00-06, 101927Z Jul 00, Security Office Digest Third Quarter 2000.

AIG 8551 00-07, 112039Z Jul 00, New AIA Security Publications.

AIG 8551 00-08, 241831Z Jul 00, USAF Foreign Disclosure Training Class.

AIG 8551 00-09, 022015Z Aug 00, AIA Security Excellence Award.

AIG 8551 10-00, 211518Z Aug 00, Recap #2 AIG 8551

AIG 8551 11-00, 162128Z Aug 00, New AIA Security Publication

2. PERSONNEL SECURITY.

2.1. MARRIAGE TO NON-U.S. CITIZENS by Mr. Lenny Martin, HQ AIA/SOPS.

Ahhhh, overseas tours! Being overseas can be an adventure. Strange surroundings, customs and culture – intriguing at least. Living amongst the local populace, you gain an appreciation for the local culture and its customs. Friendships develop. Given time, many friendships develop further into intimate relationships and love begins to blossom.

Discussions of marriage, light hearted at first, become more and more serious and frequent. Rather than getting married, a decision to "try it out first," by living together is made. A place to live is decided upon and the couple moves in together.

Time passes. The "trial" period was a success. The next step - marriage. A date picked. Vows exchanged. Preachers pray. Bells ring. Married – till death do you part.

This scenario is all well and good for those people who are not indoctrinated for access to Sensitive Compartmented Information (SCI). Not true for those who are.

The Director of Central Intelligence Directive (DCID) 6/4, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information*, states a person requiring access to SCI must be a U.S. citizen. It further states the person's immediate family must also be U.S. citizens. Immediate family is defined as "the spouse, parents, siblings, children, and cohabitant of the individual requiring SCI access."

This doesn't mean a couple with one foreign partner can't get married or even live together. It only means a stop at the unit's Security Office is required prior to marriage/cohabitation. The couple should be prepared to provide the names, addresses, citizenship and vocations of the intended spouse/cohabitant and their immediate family members. The Security Office uses the information to request authority for the couple to marry, or cohabitate, from the MAJCOM SSO.

Once the Security Office has all the requested information, authority is normally provided to the requesting Security Office within a day or two.

After marriage/cohabitation, one last visit to the Security Office is required. This time to complete a Single Agency Check (SAC) on the new spouse, or cohabitant, which is forwarded to the Defense Security Service. Dependent upon the results of the SAC, favorable or not, will determine whether or not the SCI indoctrinated person will remain eligible for access to SCI.

When making plans to get married (or live together) to a non-U.S. citizen, remember to notify the Security Office first!

2.2. I'M HOSTING A CONFERENCE, WHAT DO I NEED TO DO by MSgt Chris Forshey, HQ AIA/SOPS.

Hey security folks, what must I do if I'm responsible for sponsoring or co-sponsoring a conference or symposium involving unclassified, classified, or military critical unclassified Department of Defense (DoD) information? How much lead-time must I give your office for processing such an event?

The key to a successful conference or symposium is advanced planning by the sponsoring agent. AFI 61-205, *Sponsoring Or Co-Sponsoring, Conducting, And Presenting DoD-Related Scientific Papers At Unclassified And Classified Conferences, Symposia, And Other Similar Meetings*, outlines the requirements for hosting such events and provides a basic checklist for you to follow. Keep in mind all such actives must be approved by the Administrative Assistant to the Secretary of the Air Force (SAF/AA)(through SAF/IADV) a minimum of *6- months* in advance.

To obtain approval from SAF, you must first provide the following to your security manager:

Table 1. Submit the following to your security manager.

1. Justification for Air Force sponsorship.
2. Subject of the meeting and the scope of classified topics, including the maximum authorized classification level.
3. Expected dates and location.
4. Identity of the Air Force sponsor.
5. Names and telephone numbers of the Air Force points of contacts.
6. Draft of the proposed announcements or invitations to be sent to prospective attendees or participants.
7. Identity of any non-governmental organizations involved and full description of the type of support they are providing.
8. Justification for specific exclusion of foreign nationals, with a description of the sensitive information to be presented upon which the exclusion is based.

Your security managers will develop and implement adequate security measures, to include an access control plan for your conference needs. This information will then be coordinated through your Servicing Security Activity for conformity. After the coordination process is complete, the package will be forwarded to SAF/AA through the Disclosure Division, Office of the Deputy Under Secretary of the Air Force for International Affairs (SAF/IADV) for approval. Please do not publish formal notices or invitations until you receive approval to hold the event from SAF/AA.

The security folks have given you a basic plan to follow. Please remember 6-month lead-time is required for SAF/IADV to process your request. So, keep in mind you must provide all checklist items outlined in AFI 61-205 to your security manager prior to the 6-month period to preclude any delays in processing. We, in the security office, recommend you coordinate the conference or symposium package with protocol, security, foreign disclosure, procurement, scientific and technical information, the Air Force Information for Industry Offices, and public affairs to ensure a successful conference.

3. PHYSICAL SECURITY.

3.1. RISK MANAGEMENT...NOT JUST MORE BUZZWORDS by SMSgt Butch Faust, HQ AIA/SOX.

For the last few years the phrase "based on risk management principles" has been often used to explain why levels and methods of security exist at different locations throughout the Sensitive Compartmented Information (SCI) community. It has become a pivotal factor in administrative security for SCI. But what does risk management mean? Why was it developed? How is it implemented, and how do we as individuals support its intent? These are questions that, if understood by all, greatly support the enforcement of security standards and controls.

Let's first start with what risk management is. *It is the process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost*. Risk management effectively links security strategies and related costs to realistic threat assessments and risk levels. Three key terms that require further definition are risk, countermeasure, and cost. Risk is the potential for damage or loss of an asset.

The level of risk is a combination of two factors: 1) the value placed on an asset due to its cost or the consequence of loss, and 2) the likelihood that vulnerability will be exploited by a particular threat. Countermeasure is an action taken or a physical measure used to reduce or eliminate one or more vulnerabilities. The cost of a countermeasure may be monetary, but may also include non-monetary costs such as reduced operational efficiency, unfavorable working conditions, and political consequences. Now that we know the contributing factors of what risk management is, let's look at why it was developed in the first place.

In 1994, the Joint Security Commission identified the following problems with security policy and procedures. First, countermeasures were frequently out of balance with the threat. Second, large sums were spent on technical security within the U.S. despite a minimal level of threat. Third, procedural security measures were not always effective.

Consequently, the Commission envisioned security as a dynamic process guided by four basic principles: First, our security policies and procedures must be realistically matched to the threats we face. Second, our security practices must be consistent across the Intelligence Community to reduce inefficiencies and enable us to allocate scarce resources efficiently. Third, security standards must result in fair and equitable treatment of the members of our community. Fourth, our procedures must provide the security we need at a price we can afford.

These guiding beliefs are the foundation for efficient, but effective, security and why we practice risk management. This leads us to our final question. How do we implement risk management and what are our individual roles?

Risk management starts by using a 5-step process.

Table 2. Risk Management 5-Step Process.

1) Determine what we need to protect and appraise its value, keeping in mind our definition of value.
2) Identify the threats to our assets.
3) Identify the vulnerabilities of our assets.
4) Identify all countermeasures, costs and tradeoffs.
5) Assess the asset, threat, vulnerability and acceptable level of risk to determine what countermeasures to apply.

Risk management effectiveness continues and is enhanced when individual unit members, as well as security officials, are aware of unit assets to be protected, risks associated with those assets, and countermeasures applied to counter those risks.

Knowing what risk management is, why it came about, and your part in supporting its intent is essential in ensuring a correct balance of risk, countermeasure, and cost is appropriately applied to our national assets.

Portions of this article were abstracted from the 1994 Joint Security Commission Report.

3.2. IS YOUR INSTALLATION'S ANTITERRORISM/FORCE PROTECTION (AT/FP) PROGRAM WORKING FOR YOU? by SMSgt Butch Faust, HQ AIA/SOX.

U.S. Military members, their families, and facilities have become increasingly frequent terrorist targets over the past 25 years. Terrorist attacks have killed over 300 DoD service members and civilians and injured more than 1,000 during this period. The losses in property damage account for millions of dollars. A strong installation AT/FP program reduces the likelihood of terrorist attacks and mitigates the effects of such attacks should they occur. As an installation's tenant unit, our inputs to the program manager are vital to the AT/FP program. This program is designed to integrate security precautions and defensive measures for tenant organizations as well as the installation.

The following questions will assist you in determining whether the installation's AT/FP program and your unit's efforts are meeting requirements as outlined in DoDD 2000.12, *DoD Antiterrorism/Force Protection Program*:

Table 3. Checklist for AT/FP Program.

1. Does the installation's AT/FP program include a current local-threat assessment plan?
2. Does the installation's AT/FP program include provisions to conduct a physical security vulnerability assessment at least every three years?
3. Are there procedures to ensure personnel traveling overseas (includes travel between OCONUS, CINC, and AORs) receive Level 1 Antiterrorism Awareness Training?
4. Is Level 1 Antiterrorism Awareness Training properly documented? (NOTE: Pending modification of PC-III/MILMOD, unit ancillary training managers are required to document the full name, rank, SSN, and date of Level I training IAW AF/XOFP message 052209Z Jan 00.)
5. Does the installation's AT/FP program include the local community, inter-service, and tenant organizations to provide security, law enforcement, fire, medical, and emergency response capability in reaction to a terrorist event?
6. Have procedures been established to ensure that all military construction projects are reviewed at the conceptual stage to incorporate physical security, antiterrorist, and protective design features?

This list of questions is not fully inclusive; however, "No" answers to these questions can indicate a need for increased emphasis by the installation's AT/FP program manager and your organization. It is important to remember AT/FP responsibilities are a two-way street. It is the program manager's responsibility to ensure services are provided to your unit and your unit's responsibility to know what services to expect. Refer to DoDD 2000.12 and AFI 31-210, *The Air Force Antiterrorism/Force Protection Standards* for further information.

JIMMY R. JONES
Chief of Security